How to add script analysis to a profile to detect suspicious code and autoruns

Click ‘Configuration Templates’ > ‘Profiles’ > open a Windows profile > Click ‘Add Section’ > ‘Script Analysis’

- Script analysis improves endpoint protection by analyzing the code of a program to detect zero-day and file-less malware.

  Xcitium Client Security (XCS) uses the following two methods to analyze code:

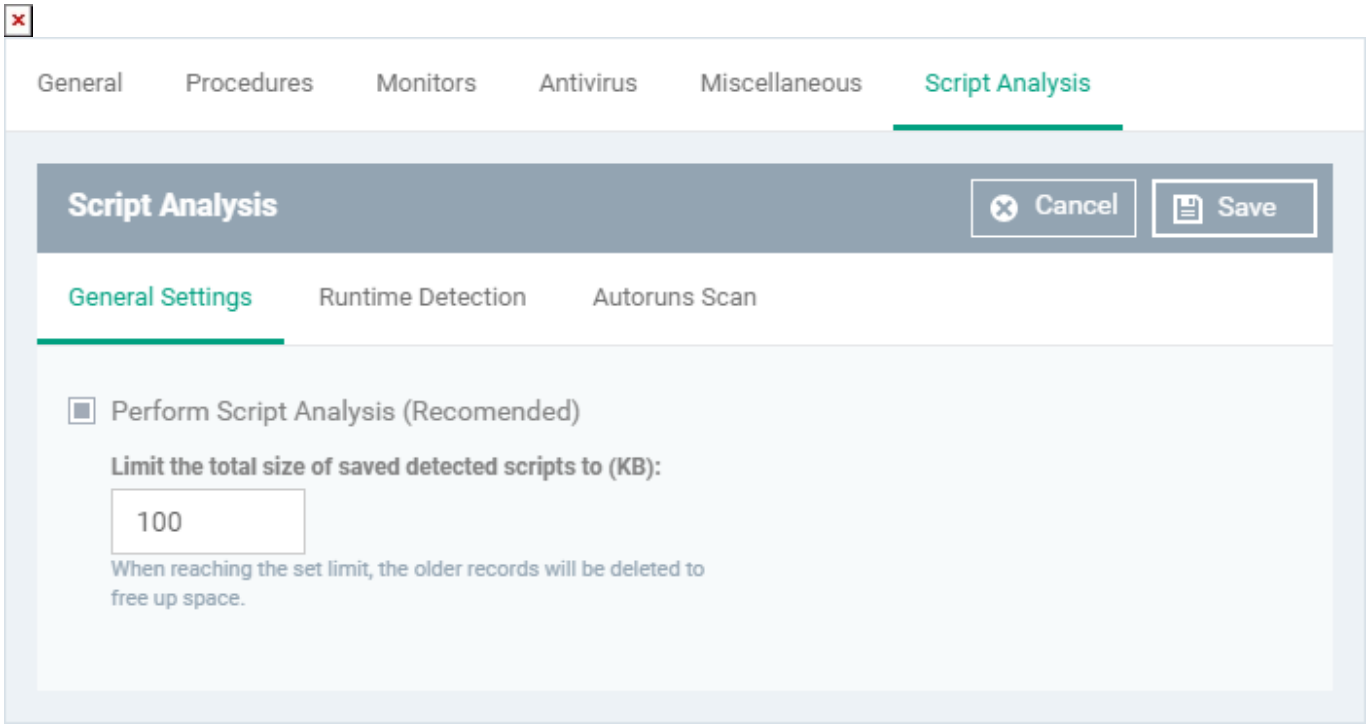
  - **Heuristic command line analysis** - Identifies files that have virus-like attributes. This lets XCS detect new, previously unknown malware.
  - **Embedded Code Detection** – Detects non-compiled, file-less code loaded to your system memory. File-less malware allows malicious actors to directly execute commands on your system.
  - See the background infromation at the end of this section if you want to know more about these technologies.

- This article explains how to add a script analysis section to a profile.

Add script analysis to a profile

- Login to Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
- Click the ‘Profiles’ tab
- Open the Windows profile applied to your target devices
  - Open the 'Script Analysis' tab

    OR
  - Click 'Add Profile Section' > 'Script Analysis', if it hasn't yet been added
- Enable script analysis under the 'General Settings' tab
- Click 'Save'



Configure script analysis

The script analysis screen has three tabs:

- General Settings - Enable script analysis and set the maximum file size which should be checked.
- Runtime Detection - Select which programs are monitored.
- Autoruns Scan - Choose programs that you want to monitor to see if they make changes to auto-run entries, Windows services and scheduled tasks.

General Settings

- **Perform Script Analysis** - Enable/Disable script analysis. An alert is generated if malicious code is found in any item. (Default = Enabled)
- **Limit the total size of saved detected scripts to** - XCS stores scripts run by managed applications for analysis. This option lets you specify the total size of stored scripts. When the set limit is reached, the older scripts are deleted automatically. (Default = 100 KB)

Runtime Detection

- Lets you select executables that should be analyzed throughout their runtime.
- You can also add custom applications that you want to protect.

Script Analysis

General Settings | Runtime Detection | Autoruns Scan

Manage the list of applications for which you would like to perform script analysis before execution.

Add | Edit | Remove | Reset to Default

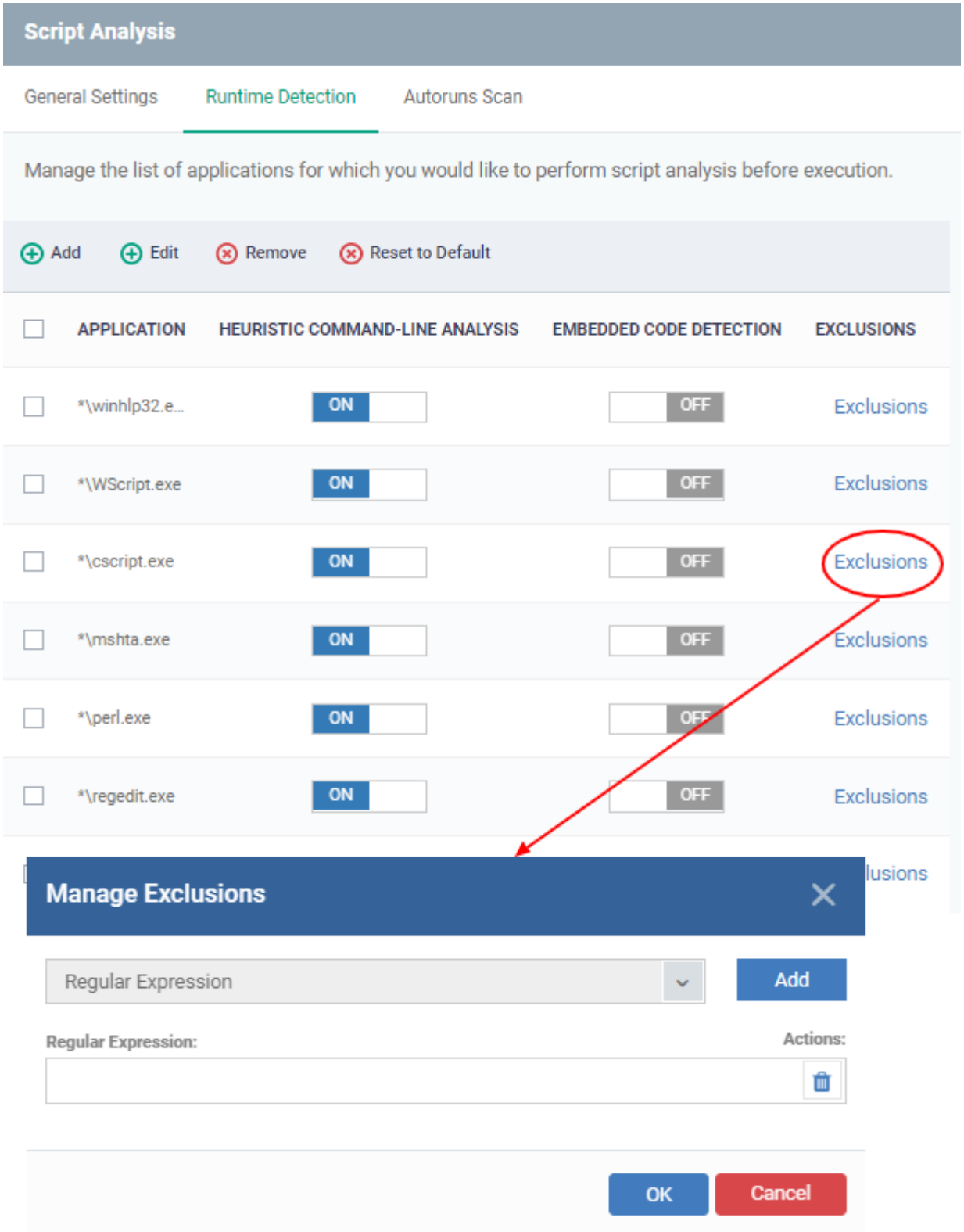
APPLICATION	HEURISTIC COMMAND-LINE ANALYSIS	EMBEDDED CODE DETECTION	EXCLUSIONS
*\winhlp32.e...	ON	OFF	Exclusions
*\WScript.exe	ON	OFF	Exclusions
*\cscript.exe	ON	OFF	Exclusions
*\mshta.exe	ON	OFF	Exclusions
*\perl.exe	ON	OFF	Exclusions
*\regedit.exe	ON	OFF	Exclusions
*\acrord32.e...	OFF	OFF	Exclusions
*\hh.exe	ON	OFF	Exclusions
*\java.exe	ON	OFF	Exclusions
*\javaw.exe	ON	OFF	Exclusions
*\cmd.exe	OFF	OFF	Exclusions
*\rundll32.exe	ON	ON	Exclusions
*\msiexec.exe	ON	OFF	Exclusions
*\regsvr32.e...	ON	OFF	Exclusions
*\powershell...	ON	ON	Exclusions
*\python.exe	ON	ON	Exclusions

    - Use the switch in the 'Heuristic Command-Line Analysis' column to enable/disable heuristic command-line analysis for each application.

    - Use the switch in the 'Embedded Code Detection' column to enable/disable embedded code detection for each application.
- Click Script Analysis > Autoruns scans > Exclusions

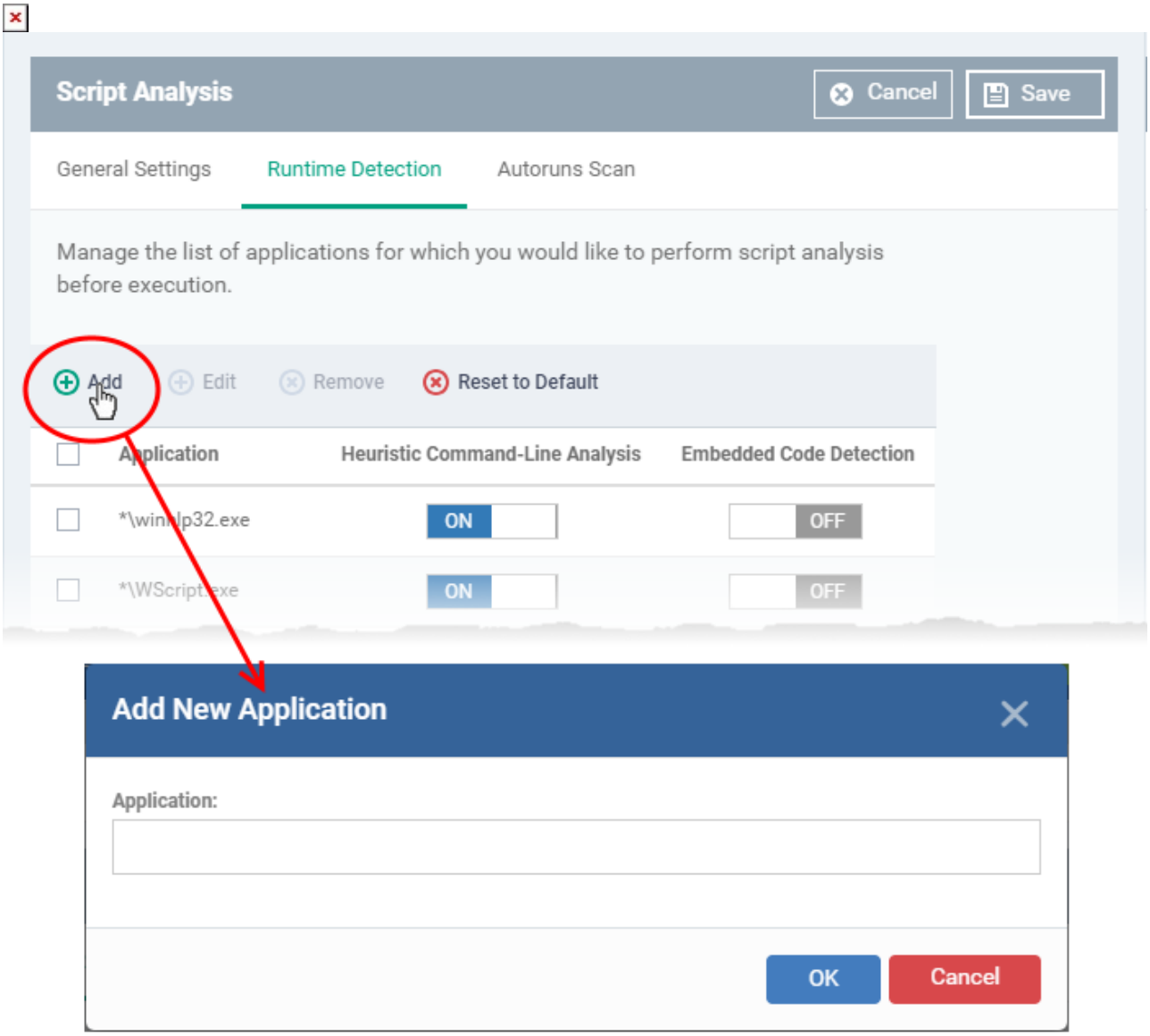
- Select an application in which you need to add an exclusion

- Click 'Add', Enter a regex, and click 'Ok' to save your changes



- This feature will exclude and log the command line detected by script analysis by defining a regular expression.
- For ex: If a malware script in the comment statement contains something that matches exclusion, that will be vulnerable and launched. This functionality will allow for the creation of malware that is focused on XCS.
- To delete the added regex click the delete icon, and then the selected regular expression will be removed.

- Click 'Add' to include a new application:



  - Enter the name of the application in the 'Add Application' dialog and click 'Add'.
  - Repeat the process to add more applications

- Click 'OK' to apply your changes.

Autoruns Scan

- Select applications that should be monitored if they make changes to autoruns, Windows services or scheduled tasks.
- You can also add custom applications which you want to monitor.
- Click the 'Autoruns Scan' tab

Script Analysis

General Settings | Runtime Detection | Autoruns Scan

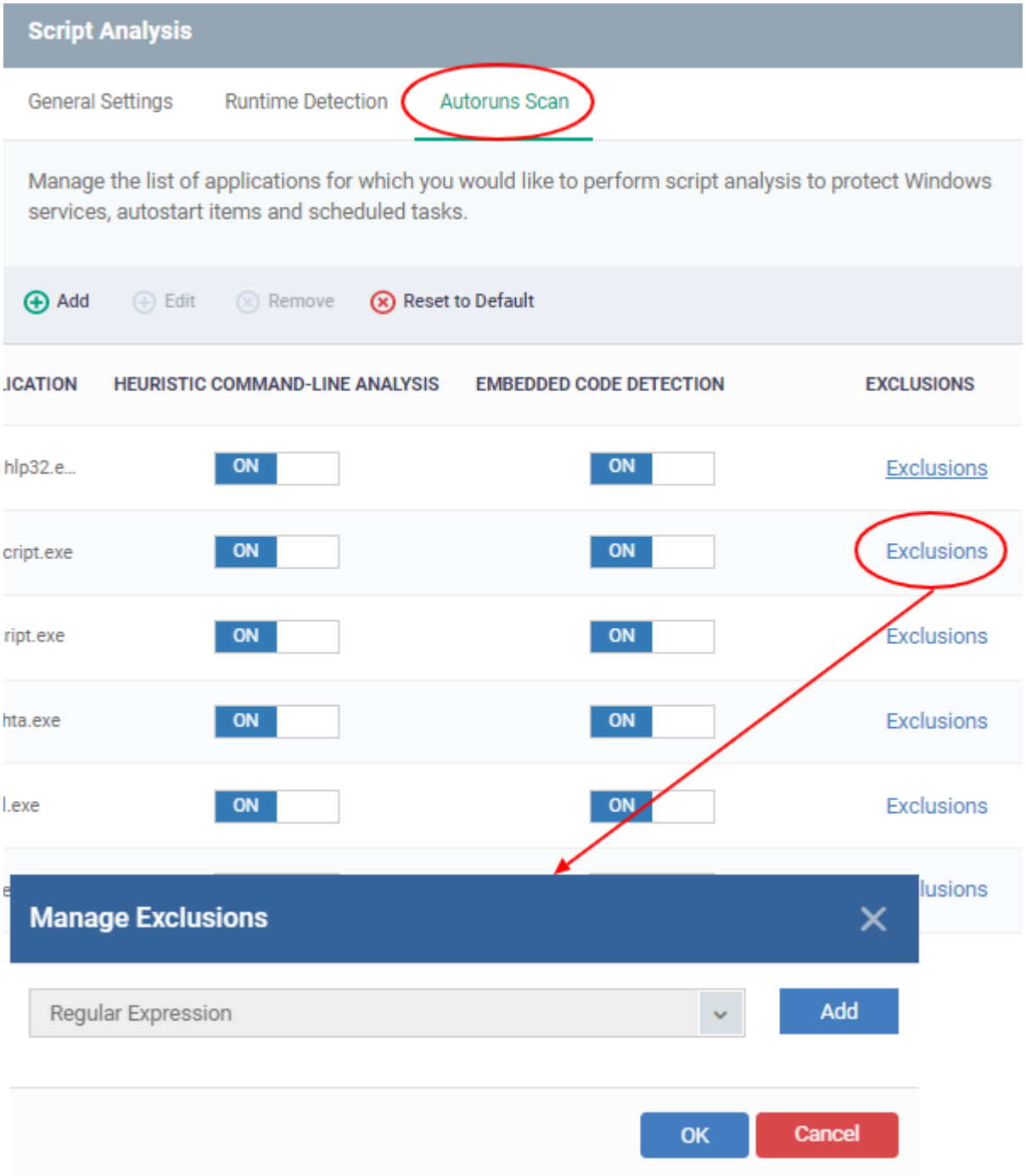
Manage the list of applications for which you would like to perform script analysis to protect Windows services, autostart items and scheduled tasks.

Add | Edit | Remove | Reset to Default

APPLICATION	HEURISTIC COMMAND-LINE ANALYSIS	EMBEDDED CODE DETECTION	EXCLU
*\winhlp32.e...	ON	ON	Excl
*\WScript.exe	ON	ON	Excl
*\cscript.exe	ON	ON	Excl
*\mshta.exe	ON	ON	Excl
*\perl.exe	ON	ON	Excl
*\regedit.exe	ON	ON	Excl
*\acrord32.e...	ON	ON	Excl
*\hh.exe	ON	ON	Excl
*\java.exe	ON	ON	Excl
*\javaw.exe	ON	ON	Excl
*\cmd.exe	ON	ON	Excl
*\rundll32.exe	ON	ON	Excl
*\msiexec.exe	ON	ON	Excl
*\regsvr32.e...	ON	ON	Excl
*\powershell...	ON	ON	Excl

- Use the switch in the 'Heuristic Command-Line Analysis' column to enable/disable heuristic command-line analysis for each application.
- Use the switch in the 'Embedded Code Detection' column to enable/disable embedded code detection for each application.

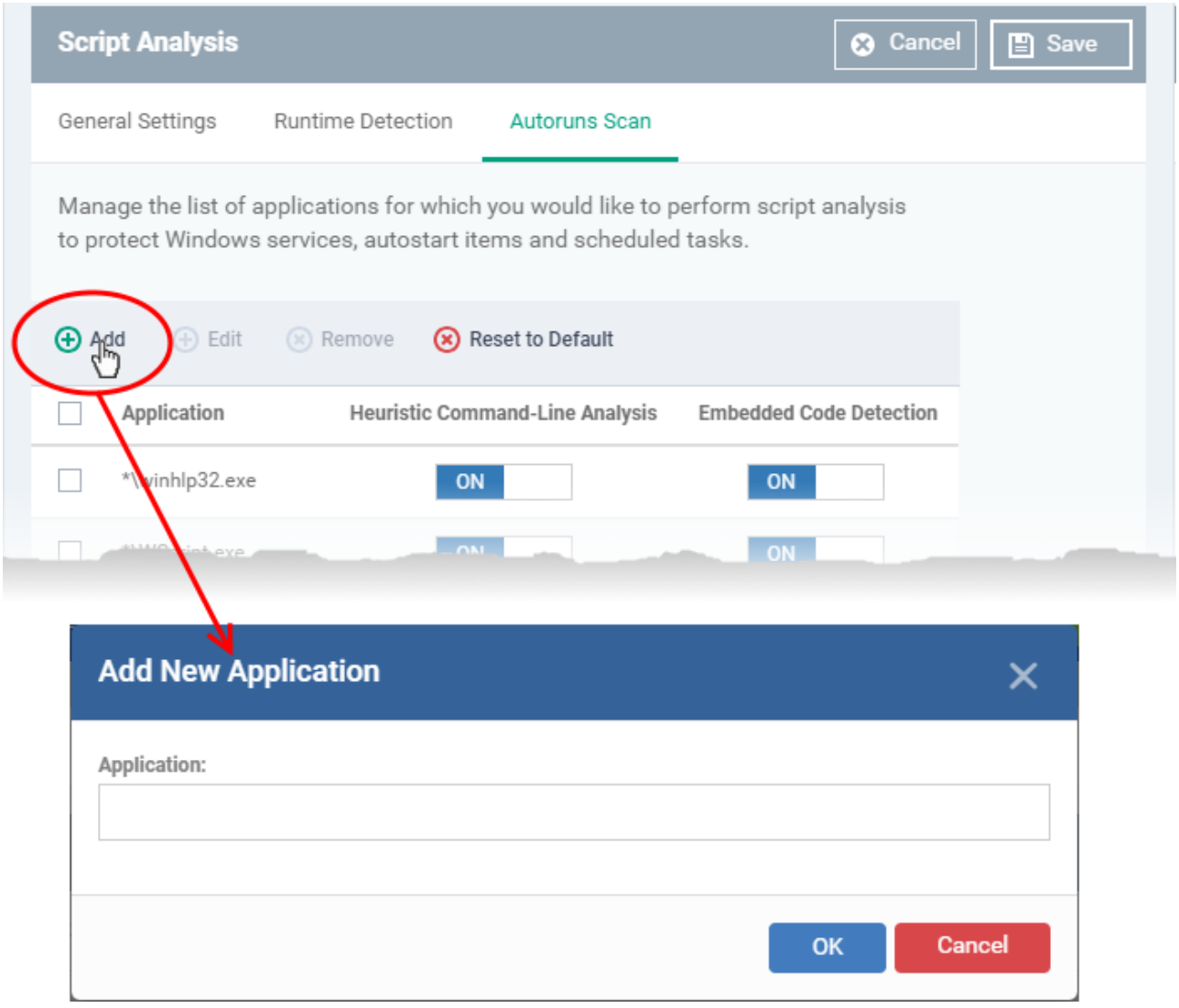
- Click Script Analysis > Autoruns Scans > Exclusions
- Select an application to which you need to add an exclusion
- Click 'Add' .Enter a regex, and click 'Ok' to save your changes



- You can exclude and log the command line detected by script analysis by defining a regular

expression. The detected but excluded items shall be able to log as 'ignored'.

- Click ‘Add’ to enter a new regular expression.
- To delete the added regex click the delete icon, and then the selected regular expression will be removed.
  ???????
- Click 'Add' to include a new application:



  - Enter the name of the application then click 'Add'.
  - Repeat the process to add more applications

- To reset the list to the default list of applications, click 'Reset to Default' on the top
- Click 'OK' to apply your changes.

Background information

Heuristic command line analysis:

- Heuristic analysis helps identify new malware by inspecting a file’s code to see if it contains code

typical of a virus.

- The system detects files that have ‘virus-like’ attributes, instead of looking for a signature that matches a signature on the blacklist.
- This allows the engine to predict new viruses - even if they are not in the current virus database.

Embedded code detection:

There are two types of executable programs:

- **Compiled** - These programs can execute on their own. Examples include .exe and .dll files.
- **Non-compiled** - These are scripts that require an interpreter program to execute them. For example, Powershell scripts (.ps1) are interpreted and executed by the Powershell program.

Embedded code detection protects you against attacks from non-compiled malware (also known as file-less malware).

- File-less malware attacks allow hackers to execute PowerShell commands on your system directly.
- These commands can be used to take control of endpoints, install ransomware, steal confidential data and more.
- File-less scripts reside in memory, so no trace remains after the computer is restarted.
- Example programs affected by these attacks are wscript.exe, cmd.exe, java.exe, and javaw.exe.
- For example, the program wscript.exe can be made to execute visual basic scripts (.vbs files) via a command similar to 'wscript.exe c:/tests/test.vbs'. When script analysis is enabled, XCS detects c:/tests/test.vbs from the command line and applies all security checks to this file.